Mr. Chairman and members of the committee: My name is Chester Hosmer; and I am a co-founder and the President and CEO of WetStone Technologies, Inc.

I would like to thank you for the opportunity to testify regarding Cybersecurity Education. This area has been, and continues to be a focal point of our work at WetStone from many perspectives. I will focus my remarks on our practical experience with Cybersecurity Education as an employer, educator, and trainer, and I will limit my focus to the areas that we are intimately involved in – digital investigation and cyber defense. I hope that our "hands on" perspective will provide an interesting frame of reference for this committee.

WetStone was established in 1998 and is headquartered in Cortland, New York. We perform advanced research and development in cybersecurity for government and corporate customers. We also develop commercial software products that aid in digital investigation and cyber defense, and we provide advanced training for digital investigators. During the past 2 years, our focus has been on cybersecurity training which includes advanced courses in Steganography and Malware Investigation, two technologies used extensively by cyber criminals. During that time we have delivered training to over 1,000 federal law enforcement agents, DoD information warriors, state and local law enforcement investigators and corporate security professionals. The demand for training in these advanced areas has grown rapidly over the past two years to the point where we are typically conducting two or three trainings per month, both in our Cortland training facility, in conjunction with cyber security conferences and at customer's onsite locations.

What knowledge and skills are currently needed in the cybersecurity workforce?

Those tasked with investigating cyber crime or defending against cyber threats require knowledge of the domain, specialized skills and practical experience. The need is currently both wide and deep. A thorough basis and understanding of investigation techniques either from a criminal justice or law enforcement background, or a formal education program is required. However, when investigating cybercrime, a strong operational and procedural technical knowledge rooted in the computer science field, is also necessary. Unfortunately, most Criminal Justice university programs are offered out of the Social Science departments at universities, where Computer Science a hard science, out of the math or computer science departments. Building programs that cross domains is quite difficult for many reasons, and the student typically lacks depth in either area, and is ill prepared for digital investigation after graduation. We are however, beginning to see an increase in specialized Computer Forensics programs which give students the background necessary for advanced digital investigation.

Many of the current investigators have come through the traditional law enforcement track and learned basic investigation techniques by working task force assignments (narcotics, homicide, child exploitation etc.). As their cases began to include more and more computer based evidence, the investigators sought training programs that would allow them to seize, extract, examine, analyze and give related testimony about digital or cyber evidence.

Many colleges and universities are attempting to meet the needs of the cyber first responder by offering evening classes or special workshops. However, the colleges and universities are not equipped to offer the advanced "hands-on" training courses needed. In many cases to properly teach these skills, special technology, dedicated laboratories, field knowledge, and extensive preparation is required. Further complicating college based offerings, is the rapid evolution of both the cyber threats and the defenses necessary to counteract them. This instability in curriculum content makes it very difficult for colleges and universities to develop programs under traditional models.

Have cybersecurity education and training programs been sufficiently flexible to respond to these needs as well as the needs of traditional and returning students?

The current state-of-the-art of cybersecurity education and training is varied. Many colleges and universities are now offering both courses and curriculums that range from Junior colleges programs offering A.A.S degrees, undergraduate education offering B.S and B.A degrees, and graduate degree programs offering both masters and doctorial degrees that relate to cybersecurity. I have personally been involved in three specific programs being offered at two colleges. At Utica College of Syracuse University, I have been privileged to teach in both the Economic Crime Investigation undergraduate program, and the Economic Crime Management Masters level program. Currently, I serve as the Director of the Computer Forensic Research and Development Center at Utica College and I guest lecture in both the computer security and computer forensic classes. At Tompkins Cortland Community College (TC3) a Junior college of the State

University of New York I had the pleasure of working with the administration and department heads to help establish the first Associates Degree program in Computer Forensics in the United States, and I continue to guest lecture in this program today.

Many commercial vendors are offering training programs that typically relate to their own specialized technology or product and service offerings. In most cases these classes are cost prohibitive for individual purchase and often place a hardship on limited department budgets. Training programs of this type vary widely in price, however a good rule of thumb is about $750 – $1,000 per day not including expenses. Advanced training courses typically run 2-5 days in duration. Investigators spend about 1-2 weeks per year on the training required to keep up to date with the state-of-the-art. Compounding the high cost of the training itself, is the time required away from the job. Those working in more rural communities must incur additional travel expenses on top of the high cost of the training. Since these costs recur every year based on the rapid changing landscape of cyber security, a minimum investment of $25,000 to $35,000 per year, per investigator is necessary. Distance learning would seem to be an obvious option that could mitigate some of these costs. This does offers a promise for the future, however, to date only a handful of cyber security training courses are offered in this manner and additional study, research and development is needed.

What are the current strengths and weaknesses in cybersecurity education and training programs?

Strengths – During the last several years new college based curriculums have been developed to address the demand for cyber security professionals. These programs are being offered at every level of secondary education, and the expertise of the faculty and curriculum development continue to rapidly advance. Options for Associates, Undergraduate and Graduate degree programs offer both new students and those wishing to advance their careers several options from which to choose. Also, many of these curriculums are offered in a "continuing education environment", allowing those currently working to participate as well.

Training offered by private companies, and conference and workshops are providing excellent content today. This type of training has many positive characteristics. First, the content tends to be well aligned with the current threats and solutions due to the competitive nature this environment offers. In addition, the quality of both the trainers and content is sound due to the demand of customers, organization members or conference participants. We see this clearly as the largest area of expansion over the past several years. Conference participants can now attend advance training course, receive college credits, take examinations for industry certifications, stay abreast of emerging trends and network with colleagues during a typical 5 day conference.

Weaknesses – Although the education programs have quickly ramped up to develop curriculums and degree offerings to help meet the needs, the graduates of these programs require significant training on practical cyber security matters after graduation, and throughout their careers. In addition, typical college and university based programs have a difficult time staying abreast of current trends. Unfortunately, in the business of cybersecurity, the trends are changing so rapidly that crafting curriculums to meet the needs is a challenge. This not only goes to the curriculum, but also the tools and technologies and expensive laboratory equipment and software necessary to expose the students to the latest methods.

The majority of the training programs currently being offered to provide practical skills by both private and non-profit organizations are non-standardized, ad-hoc and mostly difficult to qualify or assess. This makes the selection of these programs for training extremely difficult, and the satisfaction level of the attending student low. Unfortunately, due to the rapid evolution in the cyber threat, training is a recurring consideration for both new hires and veteran employees. No uniform certification process for training courses or trainers is in place today to help assess the quality and/or value of the training programs offered. Many organizations utilize colleges and universities to "accredit" their course offerings and deliver continuing education credits to those that complete the training classes. Students then have a number of CEU credits from a variety of colleges and universities with no way to combine those for a degree. In many cases students end up with 100's of hours of seemingly unrelated course credit, when in fact they have acquired more knowledge than most 4 year college students attending a traditional academic program.

Do model programs exist and, if they do, are they being adapted to meet local cybersecurity needs?

The National Security Agency (NSA) has created *The Centers of Academic Excellence in Information Assurance Education (CAEIAE)* program. Established in November 1998, this endeavor helps NSA partner with colleges and

universities across the nation to promote higher education in Information Assurance (IA). This program is an outreach effort that was designed and is operated in the spirit of Presidential Decision Directive 63 (PDD 63), the Clinton Administration's Policy on Critical Infrastructure Protection, dated May 1998. The program is now jointly sponsored by the NSA and Department of Homeland Security (DHS) in support of the President's National Strategy to Secure Cyberspace, February 2003. The goal of CAEIAE is to reduce vulnerability in our national information infrastructure by promoting higher education in information assurance (IA), and producing a growing number of professionals with IA expertise in various disciplines."[1] In New York, Pace University, Polytechnic, SUNY Buffalo, SUNY Stony Brook, Syracuse University and the U.S. Military Academy, West Point have been certified.

Numerous options for training are available at the federal level, including FBI Quantico, the Federal Law Enforcement Training Center (FLETC), the Secret Service Training Center and many others. State and local law enforcement typically with smaller budgets, receive training from private for profit or non-profit organizations such as the High Technology Crimes Investigation Association (HTCIA), InfraGard, the National White Collar Crime Center, the National Law Enforcement Training Center (NLETC) along with many others. In many cases the investigators and officers pay for membership and training out of there own pocket. At WetStone we have first hand experience with this phenomena and receive multiple requests weekly to attend our training by these individuals paying with their own funds to stay current with the emerging threats.

What partnerships should two-year and four-year colleges and universities forge with business and industry to build appropriate programs? In your opinion, is there sufficient collaboration with industry at the administration (advisory committees), faculty (return-to-industry) and student (internship) levels to accommodate rapid changes in these professional and technical areas?

The experiences over the course of my 20+ years in this industry, both in and out of the classroom have provided me with a very interesting perspective regarding not only the needs but the progress that has been made. First, I must say that the young men and women seeking education in these areas are some of the best and brightest I have had the privilege to work with. I learn more every time I enter the classroom either in an academic or training setting than I could possibly repay. During the very early days of WetStone, we launched an aggressive internship program for those working on degrees in cybersecurity. This program is still in full swing today. The idea was two fold, first to be directly involved in the education process by teaching in the classroom; and second to provide internship opportunities for students that had interests in pursuing a career in cybersecurity research and development. I am happy to report to this committee that this approach has been a stellar success. To date we have executed 14 internships in cybersecurity, involving students from every college level. Over half of these students have accepted full-time employment with our company after graduation. In addition to the internships at the college level, in June of 2003 we initiated a high school internship program for high school juniors and seniors considering a career in cybersecurity. Our first high school intern Jeff Olson of Cortland High School is with us again this summer. Jeff graduated in June and will be going on to the Rochester Institute of Technology RIT where he will be studying computer engineering. Based on the success of the high school program we are expanding this internship in the fall to include two additional high school students.

The advancement and availability of education, training and internship programs is paramount if we are to strengthen our nation's cybersecurity workforce. For example, education at the undergraduate level must include practical as well as theoretical aspects. In this field of study, the state-of-the-art is changing daily and those engaged in education must keep abreast of current trends (technological, legal and operational). In addition, I believe it is important that internships should be a requirement for those working in this field. Without functional internships students graduating will continue to lack practical skills that are a requirement for success. This recommendation should not be taken lightly. A serious commitment by the student, the college or university, and the private sector is necessary to make this endeavor successful. One metric that we have developed for our own cybersecurity internship program is the 2 for 1 rule. For every two cybersecurity interns we hire, we need to dedicate one-full time staff member to direct and mentor the interns – a significant commitment for large or small companies. In many cases employers consider only the labor cost of the interns when making an intern program decision, when in fact the cost is many times higher. However, long-term commitments are necessary, and your ability to mentor these students during their junior and senior years will pay significant dividends after graduation – as they step directly into the organization and begin producing and contributing immediately. Also, the colleges and universities are required to commit staff hours to monitor the process the internships in the field. These monitors need to be selective as to the environments that students consider – again requiring

[1] http://www.nsa.gov/ia/academia/caeiae.cfm

extensive planning and follow-up for an already overloaded schedule. However the payoff here again can be considerable. By interfacing directly with prospective employers, educators are able to identify gaps in their curriculum, get feedback as to the student's preparation, and directly improve the overall programs.

Colleges and universities must forge partnerships with both the public and private sector. In my opinion the internship model is one that should be considered. This model provides all the elements necessary to better prepare students for the workforce and to garner direct feedback throughout the lifecycle of the cyber security curriculum development. As new issues and threats are revealed, this feedback will be focused and swift. The internship opportunities also allow the colleges and universities to build relationships with employers that will better define and characterize the jobs these new cyber warriors take on. This understanding will again help shape the curriculum as a whole, along with shaping the syllabus of specific courses. One other benefit of this approach will be the access to local experts that are willing to guest lecture in the classroom. These local experts educate everyone in this environment (professors, students and colleagues) not to mention what they may learn while interacting with the next generation workforce. I realize that in writing this one may think there must be and easier way, because this sounds like hard work. Unfortunately, I'm not sure there is a silver bullet, as the responsibility for advancing the cyber security of the country should fall to everyone's shoulders. In almost all cases, we have forged these relationships – one student, one professor, one college, one department head at a time. We must all take a passionate interest in advancing our capabilities against the ever increasing cyber threat and get our hands dirty, and give back what we learn and know about every aspect of this threat. Today, the criminals and terrorists communicate and they share information about weaknesses, system vulnerabilities, our critical infrastructures, social engineering, stolen passwords, credit card numbers, malicious code and the latest cyber weapons freely and virtually unchecked over the Internet. We must do the same. And I believe education and training are the basis and the first critical step. At WetStone we adopted a quote as our company's vision in 1998. The quote came from a different time when our nation was facing a different adversary, but as often happens, the words of great men withstand the test of time. Robert Kennedy said in 1960, "If we do not on a national scale attack organized criminals with weapons and techniques as effective as their own they will destroy us." By dedicating ourselves to the transfer of knowledge in cyber security to those that are defending, or will defend us, we can train the workforce of the future and begin making a difference today.

What can the federal government do to improve cybersecurity education and build the Nation's technical workforce?

I feel that the federal government can have direct impact on the advancement of education and training in cyber security from several perspectives.

First and foremost, cyber security training and education can be made more accessible to our men and women in law enforcement who today can only advance their education and training in this area by spending their personal funds, trading their vacation time, or giving up time with their families to attend a training course that will ultimately help them defend our nation. Offering them assistance to participate in qualified education and training programs will accelerate the process for those already investing in our future and encourage those that today do not have access.

Second, incentives to colleges, universities and the private sector to create internship opportunities in cyber security can be increased. The cost required to carry out this endeavor is staggering today, however, in my opinion this is an investment that we cannot afford to overlook.

Third, national accreditation of cyber security education and training programs that would allow those to combine credits and experience to obtain higher education degrees in a flexible, fair and non-traditional form is urgently needed. We need to not only attract today's young people entering college into this field, we must also encourage those that have many years of street experience in law enforcement to gain the recognition based on their years of investment in our future. When they step on the street tomorrow, they may encounter "cyber evidence" that could in-fact hold critical information that would pre-empt a crime, a pending terrorist action, or the exploitation of a child. Their preparedness, I believe, should be our paramount concern.

I would like to thank the committee for this opportunity to present my experience, thoughts, views and perspective on cyber security education and training.